

Expansion Complexity and Linear Complexity of Sequences over Finite Fields

László Mériai, Harald Niederreiter, Arne Winterhof

Johann Radon Institute for Computational and Applied Mathematics

Austrian Academy of Sciences

Altenbergerstr. 69, 4040 Linz, Austria

e-mail: {laszlo.merai,harald.niederreiter,arne.winterhof}@oeaw.ac.at

June 22, 2016

Abstract

The linear complexity is a measure for the unpredictability of a sequence over a finite field and thus for its suitability in cryptography. In 2012, Diem introduced a new figure of merit for cryptographic sequences called expansion complexity. We study the relationship between linear complexity and expansion complexity. In particular, we show that for purely periodic sequences both figures of merit provide essentially the same quality test for a sufficiently long part of the sequence. However, if we study shorter parts of the period or nonperiodic sequences, then we can show, roughly speaking, that the expansion complexity provides a stronger test. We demonstrate this by analyzing a sequence of binomial coefficients modulo p . Finally, we establish a probabilistic result on the behavior of the expansion complexity of random sequences over a finite field.

2000 Mathematics Subject Classification: 11T71, 11Y16, 94A60, 94A55, 68Q25

Key words and phrases: expansion complexity, linear complexity, pseudo-random sequences, binomial coefficients, finite fields, cryptography

1 Introduction

For a sequence $\mathcal{S} = (s_i)_{i=0}^{\infty}$ over the finite field \mathbb{F}_q of q elements and a positive integer N , the N th linear complexity $L_N = L_N(\mathcal{S})$ is the length of a shortest

The final publication is available at Springer via <http://dx.doi.org/10.1007/s12095-016-0189-2>

linear recurrence

$$s_{i+L_N} + \sum_{\ell=0}^{L_N-1} c_\ell s_{i+\ell} = 0, \quad 0 \leq i \leq N - L_N - 1, \quad (1)$$

with coefficients $c_\ell \in \mathbb{F}_q$, which is satisfied by the first N terms of the sequence. We use the convention $L_N = 0$ if $s_0 = s_1 = \dots = s_{N-1} = 0$ and $L_N = N$ if $s_0 = s_1 = \dots = s_{N-2} = 0 \neq s_{N-1}$. The *linear complexity* $L = L(\mathcal{S})$ is

$$L(\mathcal{S}) = \sup_{N \geq 1} L_N(\mathcal{S}).$$

Note that L is finite if and only if \mathcal{S} is ultimately periodic. If T and t denote the period and preperiod of \mathcal{S} , respectively, we obviously have

$$L \leq T + t.$$

The (N th) linear complexity is a measure for the unpredictability of a sequence and thus its suitability in cryptography. A sequence with small L_N for a sufficiently large N is disastrous for cryptographic applications. However, the converse is not true. There are highly predictable sequences with large L_N , including the example $s_0 = \dots = s_{N-2} = 0 \neq s_{N-1}$. Hence, for testing the suitability of a sequence in cryptography we also have to study finer figures of merit. A recent survey on the linear complexity is given in [11].

Diem [4] introduced the expansion complexity of the sequence \mathcal{S} as follows. We define the *generating function* $G(x)$ of \mathcal{S} by

$$G(x) = \sum_{i=0}^{\infty} s_i x^i,$$

viewed as a formal power series over \mathbb{F}_q . Note the change by the factor x compared to the definition in [4]. For a positive integer N , the *N th expansion complexity* $E_N = E_N(\mathcal{S})$ is $E_N = 0$ if $s_0 = \dots = s_{N-1} = 0$ and otherwise the least total degree of a nonzero polynomial $h(x, y) \in \mathbb{F}_q[x, y]$ with

$$h(x, G(x)) \equiv 0 \pmod{x^N}. \quad (2)$$

Note that E_N depends only on the first N terms of \mathcal{S} .

We prove upper and lower bounds on E_N in terms of L_N and the smallest number t_N with $c_{t_N} \neq 0$ in (1). In particular, we show that for purely periodic sequences both figures of merit provide essentially the same quality test for the whole sequences. However, if we study only parts of the period or nonperiodic sequences, we can show, roughly speaking, that the expansion complexity provides a stronger test. We demonstrate this by analyzing linear complexity and expansion complexity of the sequence $\mathcal{A} = (a_i)_{i=0}^{\infty}$ of binomial coefficients $a_i = \binom{i+k}{k}$ modulo a prime p for some $1 \leq k \leq p-1$.

First we study ultimately periodic sequences in Section 2. Then we analyze the linear complexity and expansion complexity of the sequence \mathcal{A} in Section 3. The aperiodic case is studied in Section 4. A probabilistic result on the behavior of the expansion complexity of random sequences over a finite field is shown in Section 5.

2 Ultimately periodic sequences

Now let $\mathcal{S} = (s_i)_{i=0}^\infty$ be an ultimately periodic sequence over \mathbb{F}_q with preperiod t and period T , that is, $s_{i+t+T} = s_{i+t}$ for $i = 0, 1, \dots$. Let L be its linear complexity and recall that $L \leq T + t$. Then its generating function is a rational function

$$G(x) = \frac{f(x)}{g(x)} \quad (3)$$

with polynomials $f(x), g(x) \in \mathbb{F}_q[x]$ with $\deg(f) < L$, $\deg(g) = L - t$, and $\gcd(f(x), g(x)) = \gcd(g(x), x) = 1$, see [6, Theorem 8.40]. Note that such a sequence satisfies a linear recurrence of the form

$$\sum_{\ell=t}^L c_\ell s_{i+\ell} = 0, \quad i \geq 0,$$

with $c_L = 1$ and $c_t \neq 0$. Then we have

$$g(x) = 1 + c_{L-1}x + \dots + c_t x^{L-t}. \quad (4)$$

Lemma 1 *Let $G(x)$ in (3) be not identically zero and let $h(x, y) \in \mathbb{F}_q[x, y]$ be a nonzero polynomial of local degree d in y . Put $H(x) = g(x)^d h(x, G(x))$. If $H(x)$ is the zero polynomial, then the total degree of $h(x, y)$ satisfies*

$$\deg(h) \geq L - t + 1.$$

Proof. We write

$$h(x, y) = \sum_{i=0}^d h_i(x) y^i \in \mathbb{F}_q[x, y]$$

with $h_d(x) \neq 0$. Then $H(x) = 0$ implies

$$\sum_{i=0}^d h_i(x) f(x)^i g(x)^{d-i} = 0 \quad (5)$$

and $d \geq 1$, where we used (3). Note that $g(x) \neq 0$ by (4). Hence, $h_d(x)$ is divisible by $g(x)$ and thus of degree at least $\deg(g) = L - t$. Finally, we have $\deg(h) \geq \deg(h_d) + d \geq L - t + 1$. \square

Theorem 1 *Let \mathcal{S} be an ultimately periodic sequence over \mathbb{F}_q with preperiod t , linear complexity L , and generating function $G(x) \neq 0$. Then we have*

$$E_N(\mathcal{S}) \geq \begin{cases} L - t + 1 & \text{for } N > (L - t)(L - \min\{1, t - 1\}), \\ \lceil N / (L - \min\{1, t - 1\}) \rceil & \text{otherwise,} \end{cases}$$

and

$$E_N(\mathcal{S}) \leq L + \max\{-1, -t + 1\}.$$

Proof. Since otherwise the lower bound is trivial, we may assume $\deg(h) < N/(L - \min\{1, t - 1\})$. Then $\deg(H) \leq \deg(h)(L - \min\{1, t - 1\}) < N$ using (5) and

$$h(x, G(x)) \equiv 0 \pmod{x^N}$$

is equivalent to $H(x) = 0$. Now the lower bound follows by Lemma 1.

Choosing the polynomial

$$h(x, y) = g(x)y - f(x)$$

of degree $\deg(h) = \max\{\deg(f), \deg(g) + 1\} \leq \max\{L - 1, L - t + 1\}$, we get the upper bound. \square

Remark. For $t \leq 2$ and $N > (L - t)(L - t + 1)$ we have equality:

$$E_N(\mathcal{S}) = L - t + 1.$$

3 A sequence of binomial coefficients

For a prime p and some integer k with $1 \leq k \leq p - 1$, we study the p -periodic sequence $\mathcal{A} = (a_i)_{i=0}^{\infty}$ of binomial coefficients

$$a_i = \binom{i+k}{k} \pmod{p}, \quad i = 0, 1, \dots \quad (6)$$

First we will show that \mathcal{A} has an optimal N th linear complexity for $1 \leq N \leq 2 \min\{k + 1, p - k\}$ which suggests an optimal value of $k = (p - 1)/2$. However, since the last k sequence elements $a_{p-k}, a_{p-k+1}, \dots, a_{p-1}$ in the first period vanish, the sequence becomes more predictable with increasing k .

It turns out that the p th expansion complexity is $E_p(\mathcal{A}) = \min\{k + 2, \lceil p/(k + 2) \rceil\}$ which suggests an optimal value of $k \approx p^{1/2}$, where only the first $p - k$ sequence elements should be used in practice.

3.1 Linear complexity

Proposition 1 *We have*

$$L(\mathcal{A}) = k + 1$$

and

$$L_N(\mathcal{A}) \geq \min\{k + 1, \lceil N/2 \rceil, p - k\}.$$

Proof. Since $\binom{i+k}{k} = \prod_{j=1}^k \frac{i+j}{j}$ is a polynomial of degree k in i , we can apply the following well-known result, see [2, Theorem 8] or [9, Theorem 1], to get the value of the linear complexity: let f be a polynomial of degree $d < p$ over \mathbb{F}_p and $\mathcal{S} = (s_i)_{i=0}^{\infty}$ be the p -periodic sequence defined by $s_i = f(i)$ for $i = 0, 1, \dots$; then $L(\mathcal{S}) = d + 1$. Furthermore, $L_N(\mathcal{S}) \geq \min\{d + 1, N - d\}$ by [10, Theorem 3], which implies

$$L_N(\mathcal{A}) \geq \min\{k + 1, N - k\}.$$

Put $L = L_N(\mathcal{A})$. Since otherwise the second result is trivial, we may assume

$$L \leq \min\{k, p - k - 1\} \quad \text{and} \quad N \leq \min\{2k, p - 1\}.$$

Assume there is a linear recurrence of length L satisfied by the first N terms of \mathcal{A} , that is,

$$\sum_{\ell=0}^L c_\ell a_{i+\ell} = 0, \quad 0 \leq i \leq N - L - 1,$$

where $c_L = -1$. Note that

$$a_{i+\ell} = \binom{i+\ell+k}{k} = a_i \prod_{j=1}^{\ell} \frac{i+k+j}{i+j}.$$

With $f_\ell(x) = \prod_{j=1}^{\ell} (x+k+j)$ and $g_\ell(x) = \prod_{j=1}^{\ell} (x+j)$, we get

$$\sum_{\ell=0}^L c_\ell \frac{f_\ell(i)}{g_\ell(i)} = 0, \quad 0 \leq i \leq \min\{N - L, p - k\} - 1,$$

since $a_i \neq 0$ for $0 \leq i \leq p - k - 1$. Multiplying with $g_L(i)$, we get

$$\sum_{\ell=0}^L c_\ell f_\ell(i) \prod_{j=\ell+1}^L (i+j) = 0, \quad 0 \leq i \leq \min\{N - L, p - k\} - 1.$$

We have constructed a polynomial of degree at most L with at least $\min\{N - L, p - k\}$ zeros. Evaluating the left hand side at $i = p - L \geq p - k$, we get the value $c_L f_L(p - L) \neq 0$. Hence by Lagrange's theorem we obtain

$$L \geq \min\{N - L, p - k\}.$$

If $L \geq N - p + k$, we get $L \geq \max\{N/2, N - p + k\} = N/2$ since $N - p + k \leq L < p - k$ implies $N < 2(p - k)$. If $L < N - p + k$, we obtain $L \geq p - k$. \square

3.2 Expansion complexity

Lemma 2 *The generating function $G(x)$ of \mathcal{A} is*

$$G(x) = \frac{1}{(1-x)^{k+1}}.$$

Proof. First verify that

$$\binom{p-1-k}{i} (-1)^i \equiv \prod_{j=1}^i \frac{k+j}{j} \equiv \binom{i+k}{i} \equiv \binom{i+k}{k} \pmod{p}.$$

Then we get

$$\begin{aligned}
(1-x)^p G(x) &= (1-x^p)G(x) = \sum_{i=0}^{p-1-k} \binom{i+k}{k} x^i \\
&= \sum_{i=0}^{p-1-k} \binom{p-1-k}{i} (-x)^i = (1-x)^{p-1-k}
\end{aligned}$$

and the result follows. \square

Theorem 2 Let $\mathcal{A} = (a_i)_{i=0}^\infty$ be the sequence of binomial coefficients modulo p defined by (6) and $E_p(\mathcal{A})$ its p th expansion complexity.

For $(k+1)(k+2) < p$ we have

$$E_p(\mathcal{A}) = k+2$$

and for $(k+1)(k+2) \geq p$

$$\left\lceil \frac{p}{k+2} \right\rceil \leq E_p(\mathcal{A}) \leq \max \left\{ \left\lceil \frac{p}{k+2} \right\rceil, (k+1) \left\{ \frac{p}{k+1} \right\} \right\},$$

where $\{x\}$ is the fractional part of x , that is, $\{x\} = x - \lfloor x \rfloor$.

Proof. By Proposition 1 we have $L = L(\mathcal{A}) = k+1$. If $(k+1)(k+2) < p$ we get by Theorem 1 (with $t = 0$ since \mathcal{A} is purely periodic) the first result.

If $(k+1)(k+2) \geq p$ we have by Theorem 1

$$E_p(\mathcal{A}) \geq \left\lceil \frac{p}{k+2} \right\rceil.$$

We put

$$d = \min \left\{ \left\lceil \frac{p}{k+1} \right\rceil, \left\lceil \frac{p}{k+2} \right\rceil \right\}$$

and take

$$h(x, y) = y^d - (1-x)^{p-d(k+1)} \in \mathbb{F}_p[x, y].$$

Here we used $d \leq p/(k+1)$ since otherwise $h(x, y)$ is not a polynomial. By Lemma 2 we have $G(x) = \frac{1}{(1-x)^{k+1}}$ and thus

$$\begin{aligned}
h(x, G(x)) &= \frac{1}{(1-x)^{d(k+1)}} - (1-x)^{p-d(k+1)} = \frac{1 - (1-x)^p}{(1-x)^{d(k+1)}} \\
&= \frac{x^p}{(1-x)^{d(k+1)}} \equiv 0 \pmod{x^p}
\end{aligned}$$

since $\gcd((1-x), x) = 1$. Hence,

$$E_p(\mathcal{A}) \leq \deg(h) = \max\{d, p-d(k+1)\} = \begin{cases} d & \text{if } d = \left\lceil \frac{p}{k+2} \right\rceil, \\ p-d(k+1) & \text{otherwise,} \end{cases}$$

and the result follows. \square

4 The aperiodic case

4.1 Growth of $E_N(\mathcal{S})$ and $L_N(\mathcal{S})$

First we describe the possible growth of the nondecreasing function $N \mapsto E_N(\mathcal{S})$.

Proposition 2 *We have $E_N(\mathcal{S}) \leq E_{N+1}(\mathcal{S}) \leq E_N(\mathcal{S}) + 1$.*

Proof. If $h(x, G(x)) \equiv 0 \pmod{x^N}$, then $xh(x, G(x)) \equiv 0 \pmod{x^{N+1}}$. \square

For comparison, we state the corresponding result on the possible growth of the nondecreasing function $N \mapsto L_N(\mathcal{S})$, which is called the *linear complexity profile* of \mathcal{S} . For a proof see [5, Theorem 6.7.4], [8], or [12, Chapter 4].

Lemma 3 *If $L_N(\mathcal{S}) > N/2$, then $L_{N+1}(\mathcal{S}) = L_N(\mathcal{S})$. If $L_N(\mathcal{S}) \leq N/2$, then $L_{N+1}(\mathcal{S}) \in \{L_N(\mathcal{S}), N+1-L_N(\mathcal{S})\}$.*

4.2 Bounds

Theorem 3 *Let \mathcal{S} be a sequence over \mathbb{F}_q with generating function $G(x)$. For $N \geq 2$ let $G(x)$ satisfy*

$$G(x) \not\equiv 0 \pmod{x^N}$$

and let

$$\sum_{\ell=t_N}^{L_N} c_\ell s_{i+\ell} = 0, \quad 0 \leq i \leq N - L_N - 1,$$

be a shortest linear recurrence for the first N terms of \mathcal{S} , where $c_{L_N} = 1$ and $c_{t_N} \neq 0$. Then

$$E_N(\mathcal{S}) \geq \begin{cases} L_N - t_N + 1 & \text{for } N > (L_N - t_N)(L_N - \min\{1, t_N - 1\}), \\ \left\lceil \frac{N}{L_N - \min\{1, t_N - 1\}} \right\rceil & \text{otherwise,} \end{cases}$$

and

$$E_N(\mathcal{S}) \leq \min\{L_N(\mathcal{S}) + \max\{-1, -t_N + 1\}, N - L_N(\mathcal{S}) + 2\}.$$

Proof. Let $\mathcal{U} = (u_i)_{i=0}^\infty$ be the ultimately periodic sequence with preperiod $t = t_N$ defined by

$$u_i = s_i \text{ for } i = 0, 1, \dots, N-1$$

and

$$u_{i+L_N} = - \sum_{\ell=t}^{L_N-1} c_\ell s_{i+\ell} \text{ for } i = N - L_N, N - L_N + 1, \dots$$

Then we have $E_N(\mathcal{S}) = E_N(\mathcal{U})$ and $L_N(\mathcal{S}) = L_N(\mathcal{U}) = L(\mathcal{U})$. By Theorem 1, it remains to show that $E_N \leq N - L_N + 2$ if $L_N > (N+1)/2$. In particular, we have already proved that

$$E_N(\mathcal{S}) \leq L_N(\mathcal{S}) + 1. \tag{7}$$

If $L_N(\mathcal{S}) > (N+1)/2$, then we have $L_N(\mathcal{S}) = L_{N-1}(\mathcal{S}) = \dots = L_{N-k}(\mathcal{S}) \neq L_{N-k-1}(\mathcal{S})$ for some $0 \leq k < (N-1)/2$ since $(N+1)/2 < L_N(\mathcal{S}) = L_{N-k}(\mathcal{S}) \leq N-k$. By Lemma 3 we get $L_N(\mathcal{S}) = L_{N-k}(\mathcal{S}) = N-k - L_{N-k-1}(\mathcal{S}) \leq N-k - E_{N-k-1}(\mathcal{S}) + 1 \leq N - E_N(\mathcal{S}) + 2$ by (7) and Proposition 2, and the remaining bound follows. \square

Remarks.

- For $N \geq 2$ we have

$$E_N(\mathcal{S}) \leq \min \left\{ \left\lfloor \frac{N+3}{2} \right\rfloor, N-1 \right\},$$

where $E_N \leq N-1$ can be obtained by choosing $h(x, y) = y - \sum_{i=0}^{N-1} s_i X^i$ in (2).

- The Berlekamp-Massey algorithm does not only compute the whole linear complexity profile $L_N(\mathcal{S})$ for $N = 1, 2, \dots$, but also shortest linear recurrences satisfied by the first N terms, from which we can get t_N as well; see for example [1, 5, 8].
- We may modify Diem's definition by adding the condition that $h(x, y)$ is irreducible over \mathbb{F}_q . Without this modification $E_N(\mathcal{S})$ may depend only on the first N_0 terms of \mathcal{S} for some $N_0 < N$. More precisely, assume that all $h(x, y) \neq 0$ of minimal degree satisfying (2) are of the form $h(x, y) = h_1(x, y)h_2(x, y)$ with nonconstant polynomials $h_1(x, y)$ and $h_2(x, y)$ over \mathbb{F}_q . Then $h_1(x, G(x)) \equiv 0 \pmod{x^{N_1}}$ and $h_2(x, G(x)) \equiv 0 \pmod{x^{N_2}}$ for some $1 \leq N_1, N_2 < N$ with $N = N_1 + N_2$, and so $E_N(\mathcal{S})$ depends only on the first $N_0 = \max\{N_1, N_2\}$ terms of \mathcal{S} . However, using only irreducible polynomials would cause serious modifications in the algorithm suggested in [4, Section 5].
- We have $E_{N_1+N_2} \leq E_{N_1} + E_{N_2}$ if $G(x) \not\equiv 0 \pmod{x^{\min\{N_1, N_2\}}}$. Indeed, if $h_1(x, G(x)) \equiv 0 \pmod{x^{N_1}}$ and $h_2(x, G(x)) \equiv 0 \pmod{x^{N_2}}$ with nontrivial polynomials $h_1(x, y)$ and $h_2(x, y)$, then $h(x, G(x)) \equiv 0 \pmod{x^{N_1+N_2}}$.
- Let p be the characteristic of \mathbb{F}_q . For $N \geq 2$ let k be the nonnegative integer with $p^k \leq N-1 < p^{k+1}$. Then we have $E_N \leq \lfloor (N-1)/p^k \rfloor p^k$ taking $h(x, y) = y^{p^k} - \sum_{i=0}^{\lfloor (N-1)/p^k \rfloor} s_i x^{ip^k}$, which improves $E_N \leq (N+3)/2$ in some cases.

5 A probabilistic result

Let μ_q be the uniform probability measure on \mathbb{F}_q which assigns the measure $1/q$ to each element of \mathbb{F}_q . Let \mathbb{F}_q^∞ be the sequence space over \mathbb{F}_q and let μ_q^∞ be the complete product probability measure on \mathbb{F}_q^∞ induced by μ_q . We say that

a property of sequences $\mathcal{S} \in \mathbb{F}_q^\infty$ holds μ_q^∞ -almost everywhere if it holds for a set of sequences \mathcal{S} of μ_q^∞ -measure 1. We may view such a property as a typical property of a random sequence over \mathbb{F}_q .

Theorem 4 *We have*

$$\liminf_{N \rightarrow \infty} \frac{E_N(\mathcal{S})}{N^{1/2}} \geq 1 \quad \mu_q^\infty\text{-almost everywhere.}$$

Proof. First we fix ε with $0 < \varepsilon < 1$ and we put

$$b_N = \left\lfloor (1 - \varepsilon)^{1/2} N^{1/2} \right\rfloor \quad \text{for } N = 1, 2, \dots \quad (8)$$

Then $b_N \geq 1$ for all sufficiently large N . For such N put

$$A_N = \{\mathcal{S} \in \mathbb{F}_q^\infty : E_N(\mathcal{S}) \leq b_N\}.$$

Since $E_N(\mathcal{S})$ depends only on the first N terms of \mathcal{S} , the measure $\mu_q^\infty(A_N)$ is given by

$$\mu_q^\infty(A_N) = q^{-N} \cdot \#\{\mathcal{S} \in \mathbb{F}_q^N : E_N(\mathcal{S}) \leq b_N\}. \quad (9)$$

According to [4, Proposition 7], \mathcal{S} is uniquely determined by its first b_N^2 terms. It follows therefore that

$$\#\{\mathcal{S} \in \mathbb{F}_q^N : E_N(\mathcal{S}) \leq b_N\} \leq q^{b_N^2}.$$

It follows thus from (8) and (9) that $\mu_q^\infty(A_N) \leq q^{-\varepsilon N}$ for all sufficiently large N . Therefore $\sum_{N=1}^\infty \mu_q^\infty(A_N) < \infty$. Then the Borel-Cantelli lemma (see [3, Lemma 3.14] and [7, p. 228]) shows that the set of all $\mathcal{S} \in \mathbb{F}_q^\infty$ for which $\mathcal{S} \in A_N$ for infinitely many N has μ_q^∞ -measure 0. In other words, μ_q^∞ -almost everywhere we have $\mathcal{S} \in A_N$ for at most finitely many N . It follows then from the definition of A_N that μ_q^∞ -almost everywhere we have

$$E_N(\mathcal{S}) > b_N > (1 - \varepsilon)^{1/2} N^{1/2} - 1$$

for all sufficiently large N . Therefore μ_q^∞ -almost everywhere,

$$\liminf_{N \rightarrow \infty} \frac{E_N(\mathcal{S})}{N^{1/2}} \geq (1 - \varepsilon)^{1/2}.$$

By applying this for $\varepsilon = 1/r$ with $r = 1, 2, \dots$ and noting that the intersection of countably many sets of μ_q^∞ -measure 1 has again μ_q^∞ -measure 1, we obtain the result of the theorem. \square

Theorem 4 shows that, for random sequences \mathcal{S} over \mathbb{F}_q , the expansion complexity $E_N(\mathcal{S})$ grows at least at the rate $N^{1/2}$ as $N \rightarrow \infty$. It may be conjectured that this is the exact order of magnitude of $E_N(\mathcal{S})$ for random sequences \mathcal{S} over \mathbb{F}_q .

Acknowledgements

The authors wish to thank Claus Diem for a hint which led to an improvement of the constant in Theorem 4.

The first and the third author are partially supported by the Austrian Science Fund FWF Project F5511-N26 which is part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".

References

- [1] Berlekamp, E.R.: Algebraic coding theory. McGraw-Hill Book Co., New York-Toronto, Ont.-London (1968)
- [2] Blackburn, S.R., Etzion, T., Paterson, K.G.: Permutation polynomials, de Bruijn sequences, and linear complexity. *J. Combin. Theory Ser. A* 76, no. 1, 55–82 (1996)
- [3] Breiman, L.: Probability. SIAM, Philadelphia, PA, (1992)
- [4] Diem, C.: On the use of expansion series for stream ciphers. *LMS J. Comput. Math.* 15, 326–340 (2012)
- [5] Jungnickel, D.: Finite fields: Structure and arithmetics. Bibliographisches Institut, Mannheim (1993)
- [6] Lidl, R., Niederreiter, H.: Finite fields. *Encyclopedia of Mathematics and its Applications*, 20. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA (1983)
- [7] Loève, M.: Probability theory, 3rd ed. Van Nostrand, New York (1963)
- [8] Massey, J.L.: Shift-register synthesis and BCH decoding. *IEEE Trans. Information Theory* IT-15, 122–127 (1969)
- [9] Meidl, W., Winterhof, A.: Linear complexity and polynomial degree of a function over a finite field. In: *Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001)*, pp. 229–238, Springer, Berlin (2002)
- [10] Meidl, W., Winterhof, A.: On the linear complexity profile of explicit nonlinear pseudorandom numbers. *Inform. Process. Lett.* 85, no. 1, 13–18 (2003)
- [11] Meidl, W., Winterhof, A.: Linear complexity of sequences and multisequences. In: Mullen, G.L., Panario, D. (eds.) *Handbook of finite fields*, pp. 324–336, CRC Press, Boca Raton, FL (2013)
- [12] Rueppel, R.A.: Analysis and design of stream ciphers. *Communications and Control Engineering Series*. Springer, Berlin (1986)